FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1342193-0

Total Deleted Page(s) = 1
Page 4 ~ b7D;

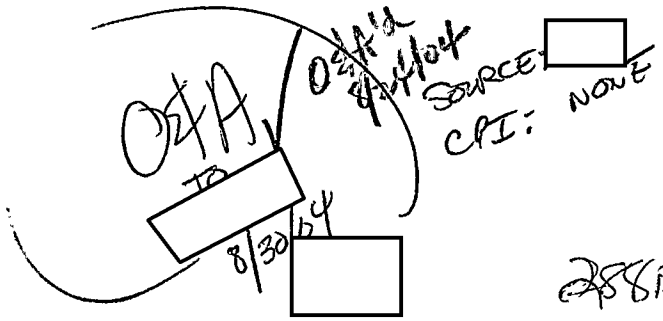
XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

288A-KX-69887-1

SSRA [ ]

b6
b7C

232 [redacted] 02 ec



[redacted]

_ SSRA

b6
b7C
b7D

288A-KY-69887-2

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/19/2004

To: Cyber **Attn:** SSA [redacted]
C3IU/Computer Intrusion
Section/5931

New York **Attn:** SA [redacted]
Squad [redacted]

From: Knoxville
Squad 8, Chattanooga RA
Contact: [redacted]

Approved By: Clark R Joe [redacted]

Drafted By: [redacted]

Case ID #: 288A-KX-~~NEW~~ 69987 (Pending)

Title: CRIMETHINC;
SmartTech Corp. - Victim;
Computer Intrusion;

Synopsis: Open and assign case to Special Agent (SA) [redacted] Update both New York and Cyber Divisions of the status of the investigation and the opening of this case. Knoxville Division considers the lead as covered.

Reference: 288B-NY-289354 Serial 10
266A-OM-49939 Serial 4
66F-HQ-A1275997 Serial 418
66F-HQ-C1384970 Serial 12611

Details: Knoxville is opening the captioned case regarding hacktivists who seek to disrupt the Republican National Convention (RNC) using electronic civil disobedience. Information provided to the FBI on 7/26/2004 and posted on different internet websites indicates that "hactivists" are attempting to disrupt the certain websites during the Republican National Convention (RNC). The following websites have been identified as targets [redacted]

[redacted] However, this email address is no

longer enabled and appears to have been disabled on or about August 17, 2004. It is unknown at this time the reason this account was disabled.

The ip-address for the [redacted] (Mail Server) records of [redacted] are all within the [redacted] network, which is registered to [redacted] which is leased from [redacted] which owns the ip range of [redacted] Writer has contacted [redacted] and determined that [redacted] does lease these aforementioned ip addresses and that it is very likely that the mail server is located at [redacted] facilities in [redacted] The technical support person was unable to confirm the location of the equipment but was fairly confident that the equipment was located in [redacted] facilities. b7E

The last three nodes of a trace route for the ip address [redacted] one of the [redacted] record for [redacted] returns the following information:

[redacted]

These records indicate that the mail server at [redacted] is one hop from the [redacted] equipment which is located in [redacted] It is therefore highly likely that this mail server is located in the same facility. Writer connected to port [redacted] on [redacted] and verified that it is a mail server.

The owner of the subnet [redacted] is listed at [redacted] as [redacted] Contact information for this subnet is listed as [redacted], telephone [redacted] However the domain name [redacted] is registered to [redacted] The contact information for this domain name is listed as [redacted] telephone number [redacted] The Technical Contact for this domain is [redacted]

The information for [redacted] is listed at [redacted] as [redacted] Contact information for this domain is listed as [redacted] telephone [redacted]

The Knoxville Division has visited the website [redacted] which describes the entire plan of action to disrupt the RNC and other website which reference the aforementioned site or the disruption plan.

The information for [redacted] is listed at [redacted] as:
Owner:
Address:
City:
PCode:
Country:

b7E
b6
b7C
b7E

The information for [redacted] is listed at [redacted] as:
Address:
email:
Phone:

b6
b7C
b7E

Writer has contacted [redacted] (Protect Identity), [redacted] Writer will be forwarding [redacted] to SA [redacted] NYO for analysis.

b6
b7C
b7D
b7E

[redacted] was aware of the efforts to attack the websites [redacted] during the RNC. They closely monitor their network and have banned traffic from most of Asia to those sites. They have a great deal of logging enabled along with redundant servers with load balancing and multiple high speed (OC3) connections to the internet. The web page is currently utilizing dynamic pages, however the web pages can individually be quickly changed to static HTML pages. This would be done if the amount of web traffic increase to the level where the back-end database cannot keep up with the page requests. [redacted] is concerned about this attack due to the great publicity on the internet for this event.

b6
b7C
b7D

Assistant United States Attorney (AUSA) [redacted] Eastern District of Tennessee, has advised writer the activities by those individuals who have created the site at [redacted] utilizing the email account [redacted] have conspired to violate Title 18, Section 1030 a(5)(A)(i) and he has committed to prosecuting those responsible, if they can be identified. Furthermore, AUSA [redacted] will review the activities of the hacktivists who seek to disrupt the RNC and determine at a later date if these actions are in violation of Title 18, U.S.C.

b6
b7C
b7E

To: Knoxville From: Knoxville
Re: 288A-KX-NEW, 08/19/2004

Section 1030, Fraud and related activity in connection with computers.

It is noted that the New York Division provided the Knoxville Division with the following information: An anarchist group using the pseudonym CRIMETHINC, released plans to coordinate hacking attempts directed at the RNC. CRIMETHINC will be presenting at a DefCon session, in Las Vegas, NV on 7/31/2004, titled "Electronic Civil Disobedience and the Republican National Convention". In the session, CRIMETHINC will discuss the theory of "hactivism" and the use of hacking to fight for social justice by placing pressure on corporations and the government to change their attitudes and policies. The session will also explore the history of ECD, suggestions for running your own ECD Campaign and explaining how participants can take part in the upcoming ECD campaign targeting the RNC. CRIMETHINC listed as targets all corporate right wing websites including government, military and news services. Specifically, CRIMETHINC urges hactivists to flood communications systems, disrupt financial systems, deface websites, and do anything politically motivated that would achieve mass attention.

Set Lead 1: (Discretionary)

NEW YORK

AT NEW YORK

Continue to forward any information collected during your investigation concerning the web site [redacted] and/or the email account [redacted] b7E

Set Lead 2: (Info)

CYBER

AT C3IU

Read and Clear.

♦♦

288A - KK - 69887

[redacted]SRA

b6
b7C

288A-KK-69887-1

[redacted] b6 b7C

From: [redacted]
To:
Sent: Friday, September 03, 2004 6:35 PM
Subject: FW: Hacktivists use Corporate Credit Cards to Donate to Humanitarian and Civil Liberties Groups

-----Original Message-----
From [redacted] [mailto [redacted]
Sent: Sunday, August 29, 2004 5:07 PM
To [redacted]
Subject: Hacktivists use Corporate Credit Cards to Donate to Humanitarian and Civil Liberties Groups

Hacktivists use Corporate Credit Cards to Donate to Humanitarian and Civil Liberties Groups

Online protesters launch electronic civil disobedience campaign against the Republican National Convention

Hacktivists have launched an online protest against the Corporate Machine by stealing hundreds of credit cards from major news services and have made over $2400 in donations to various humanitarian and civil liberties organizations including the Sierra Club, Save The Children, Animal Protection Institute, and more. This action is part of a broader electronic civil disobedience campaign against the Republican National Convention to coincide with the massive demonstrations in NYC. Speaking out against corporate control of major news services, the war in Iraq, and the GOP's exploitation of New York to further their political agenda, these hackers are pioneering the internet as a new medium of protest.

Either the credit card corporations are going to have to spend tens of thousands of dollars in lawyer and investigation fees to track down and retrieve a mere few hundred dollars per account, or these humanitarian organizations are going to get their donations. We'll have to see whether Corporate America is heartless enough to take money away from hungry children, AIDS victims and the homeless and give it straight to law enforcement, attorneys and the banks.

Modern day hacktivism: stealing from the rich ruling classes and giving to the poor and needy!

The use of hacking skills to fight for social justice and economic equality is known as ELECTRONIC CIVIL DISOBEDIENCE. It is a non-violent protest tactic that disrupts the corporate machine while causing no physical harm to people or property. By merely shifting data around in the right directions, the people are able to put direct pressure on politicians and corporations.

The GOP thinks that they can rape the city of New York to further their political agenda of endless war and attacks on our civil liberties. More than a million people will descend upon the city to declare that the Republicans are not welcome,

and we will use whatever means at our disposal to disrupt their convention - on the streets and on the net.

Earlier this week, other hacktivists have defaced ProtestWarrior's website, an extremist right-wing fascist group who infiltrates and attacks peace and social justice activist groups. The home/cell phone numbers, addresses, and passwords of the main organizers were posted along with a statement condemning their defense of the war in Iraq, the Bush Administration, and more.

We are encouraging people to participate in this campaign by joining the global electronic sit-in on the Republican Party. If enough people run the flood tools available on our campaign website, we are able to overflow GOP servers with so much traffic that it will render it unable to respond to any additional web requests.

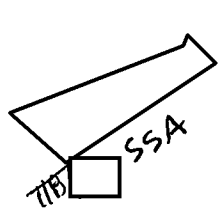
Electronic Civil Disobedience against the Republican National Convention!

http://phil.ist-backup.de/rncelectronic/

Charities that have received donations include:
tscf.org
miracleflights.org
netaid.org
lcanimal.org
fh.org
savethechildren.org
api4animals.org
chrf.org

--

b6
b7C



8/[redacted]/252[redacted]01.302

288A-KX-69887- 4

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/08/2004

Special Agent (SA) [redacted] conducted the following online investigation: b6 b7C

SA [redacted] conducted an internet text search for [redacted] which provided the following information. b6 b7C b7E

A web article titled "Interview with a Hacker", dated August 31, 2004, was posted on the web site WWW.SLANTPOINT.COM.

[redacted] b7E

SA [redacted] has attempted to contact [redacted] to get a copy of this conversation and his knowledge of who the owner of [redacted] is. The web site [redacted] was hacked by a group and then the personal information for this site was posted on the internet at a different site. [redacted] the web site [redacted] b6 b7C b7E

Investigation on 9/8/2004 at Chattanooga, Tennessee

File # 288A-KX-69887 Date dictated 9/8/2004

by SA [redacted] b6 b7C

b6
b7C

251 [redacted] 01.302

[redacted] SA

Ø98A-KX-69987-5

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/07/2004

b6
b7C
b7D
b7E

An individual, who is not is a position to testify, provided the following information:

On or about [redacted] a large number of website requests were received from the ip address [redacted] This ip address was traced back to either Detroit, MI or Philadelphia, PA and operated by [redacted]

(X)

[redacted]

Investigation on 8/19/2004 at Chattanooga, Tennessee

b3
b6
b7C
b7D
b7E

[redacted]

File # 288A-KX-69887 Date dictated 9/7/2004

by SA [redacted]
SA

[redacted] SSA

b6
b7C

8[redacted]/251[redacted] 02.302

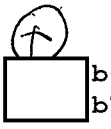
999A-RX-609887-6

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/07/2004

An individual, who is not is a position to testify, provided the following information:

On or about August 20, 2004, a large number of website requests for the web page [redacted] on the [redacted] website were received from the ip address [redacted] This ip address was traced back to [redacted] somewhere in the general area of Washington, DC. b7E



b6
b7C

Investigation on 8/19/2004 at Chattanooga, Tennessee

[redacted]

File # 288A-KX-69887 Date dictated 9/7/2004

by SA [redacted]

b3
b6
b7C
b7D
b7E

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 288A-KX-69887

633 Chestnut St.
Chattanooga, Tennessee 37450
March 15, 2005

Honorable Harry S. Mattice, Jr.
United States Attorney
1110 N. Market Street
Suite 300
Chattanooga, Tennessee 37402

Attention: [redacted] b6 b7C
Assistant United States Attorney (AUSA)

RE: CRIMETHINC;
SmartTech Corp. - Victim;
Computer Intrusion;

Dear [redacted]

The purpose of this letter is to confirm a conversation on March 14, 2005 between Special Agent (SA) [redacted] of the Chattanooga Office of the Federal Bureau of Investigation (FBI) and AUSA [redacted] in which the following facts were discussed:

During the United States Presidential Election in 2004, an individual or group named "CrimeThincInc" made overt threats on the internet to restrict or deny access to specific political web sites. It requested that individuals run a program with, in their words, would cause "civil disobedience" during the Republican National Convention. Based on this information and with the help of the New York Office of the Federal Bureau of Investigation, attempts were made to identify the individuals who posted these messages on the internet.

Since the person who posted the message on the internet appears to be overseas and has not been identified, and the since the convention passed without incident from this threat, AUSA [redacted] advised that he would not pursue federal action for violation of Title 18, U.S.C. Section 1030, Fraud and related activity in connection with a computer.

No further investigation is anticipated in this matter. The FBI will close this case accordingly. If there are any

(05095[redacted]04.ltr)

SSRA [redacted]

Close 4/7/05 [redacted]

288A-KX-69887-7

further questions, please contact SA [redacted] at [redacted]

b6
b7C

Sincerely,

R. Joe Clark
Special Agent in Charge

by: [redacted]
Supervisory Special Agent

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/07/2005

To: Knoxville

From: Knoxville
Squad 8, Chattanooga RA
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-KX-69887 (Pending)

Title: CRIMETHINC;
SMARTTECH CORP. - VICTIM;
COMPUTER INTRUSION;

Synopsis: To close investigation.

Details: A declination of prosecution was received from Assistant United States Attorney [redacted] United States Attorney's Office, Eastern District of Tennessee, Chattanooga, Tennessee.

All evidence and other collected items were properly disposed of by writer.

Based upon the above information and on the fact that no other outstanding issues related to this investigation exist, writer recommends that this investigation be closed.

(05097[redacted]02.ec)

4/8/05

Pull file.

288A-KX-69887-8